From: SANS Institute
To: ndaigle@bakersfieldpd.us
Subject: SANS NewsBites Vol. 19 Num. 65 : Cybersecurity: The Hottest New Major In College; Not Enough Hands-On, Security Training in College; Computer Science Education Shortchanges US Students
Date: Friday, August 18, 2017 11:36:28 AM

View this email as a web page

August 18, 2017 Vol. 19, Num. 65

Top of The News

- Cybersecurity: The Hottest New Major In College
- Not Enough Hands-On, Security Training in College
- International Programming Olympiad Coach: U.S. Computer Science Education Shortchanges US Students

Cybersecurity Training Update

SANS Network Security 2017 | Las Vegas, NV | September 10-17

SANS Tampa-Clearwater 2017 | September 5-10

SANS San Francisco Fall 2017 | September 2-10

The Rest of the Week's News

- Legislators Call for Investigation into FCC's Claim It Was DDoSed
- Car Safety Vulnerability Lies in the Way CAN Handles Error Messages
- ShadowPad Supply Chain Attack Affects NetSarang Software
- Tech Companies File Amici Brief in Support of Warrants for Cell Phone Data
- Maersk Details NotPetya Losses
- Ukrainian Hacker is Now FBI Witness
- Carnegie Mellon CERT's Guide to Coordinated Vulnerability Disclosure
- NIST Releases Security and Privacy Controls Draft
- Eight Chrome Extensions Hijacked
- Cyberespionage Group Targeting US Defense Companies
- Malicious PowerPoint Delivered in Spear Phishing Campaign Infected Machines with RAT

Internet Storm Center Tech Corner

SANS London September 2017 | September 25-30

SANS Rocky Mountain Fall 2017 | Denver, CO | September 25-30

SANS Baltimore Fall 2017 | September 25-30

SANS Data Breach Summit & Training | Chicago, IL | Sept.25-Oct. 2

SANS Phoenix-Mesa 2017 | October 9-14

SANS October Singapore 2017 | October 9-28

SANS Tysons Corner Fall 2017 | Tysons Corner, VA | October 14-21

Secure DevOps Summit & Training | Denver, CO | October 10-17

SANS OnDemand and vLive Training
Get an iPad Pro (10.5") with Smart Keyboard, an HP Chromebook 13 G1 or take $350 Off OnDemand or vLive Training when you register by August 30!

Single Course Training
SANS Mentor and Community SANS

View the full SANS course catalog

Free technical content sponsored by Barkly

Ransomware continues to experience record growth in 2017. Traditional solutions aren't enough and can't keep up with hundreds of thousands of new malware versions created daily. In this webcast, you will learn the three strategies Avidia Bank implemented to shut out today's sophisticated threats and how you can apply them to protect your own organization: **Register:** https://www.sans.org/info/197610

Top of the News

Cybersecurity: the Hottest New Major In College

(August 15, 2017)

Large numbers of US colleges have added undergraduate cybersecurity majors, cybersecurity concentrations to other majors, and master's degree programs in cybersecurity. Most colleges, however, do not know what to teach, and many are teaching students only how to admire the cybersecurity problem, but not how to fix it. Further, computer science graduates don't learn secure coding or other technical cybersecurity topics. None of the top ten undergraduate computer science and engineering programs at American universities (as ranked by the U.S. News & World Report) required its students to take a cybersecurity course in order to graduate.

Read more in:

- **www.villagevoice.com**: How Cybersecurity Became 2017's Hot New Major

Not Enough Hands-On, Security Training in College

(August 17, 2017)

According to a survey from Veracode, 70 percent of DevOps specialists say they did not receive adequate hands-on training while in college. Most said that they did the majority of their practical learning on the job. The DevSecOps Global Skills Survey comprises responses from 400 DevOps professionals from around the world. Eighty percent of those responding said they did not have adequate cybersecurity skills when entering the workforce. And 85 percent say they are somewhat or not at all prepared to deliver software as quickly as DevOps usually required.

Read more in:

- **www.darkreading.com**: 70% of DevOps Pros Say They Didn't Get Proper Security Training in College

USA Computing Olympiad Coach: U.S. Computer Science Education Shortchanges American Students

(August 2017)

Dr. Rob Kolstad, who coached the USA teams in the International Computing Olympiad for 20 years, explains how US computer science education has gone off track, why and how Russia's students are much better prepared to excel in cybersecurity, and approaches to turning the situation around.

Read more in:

- **www.sans.org**: How Can America's Students Compete Against Russia's Hackers? (PDF)

Sponsored Links

LNSS Labs finds many NGFWs are vulnerable to evasions. Test your firewall defenses against Evasions https://www.sans.org/info/197615

Dave Shackleford talks about how automated threat analysis is key to turning millions of raw data points into actionable intelligence. https://www.sans.org/info/197620

Join John Pescatore & E8 Security to learn how studying the behavior of people and machines shows what's normal and what may pose a risk to your organization. https://www.sans.org/info/197625

The Rest of the Week's News

Legislators Call for Investigation into FCC's Claim It Was DDoSed

(August 17, 2017)

Two US legislators are calling for an independent investigation into the Federal Communications Commission's (FCC's) claim that it suffered a distributed denial-of-service (DDoS) attack in early May. The FCC has not released documentation of the attack, leading legislators to question "the state of cybersecurity at the FCC - questions that warrant an independent review."

Read more in:

- **arstechnica.com**: FCC's claim that it was hit by DDoS should be investigated, lawmakers say
- **fcw.com**: Dems want more data on FCC DDoS attacks
- **www.nextgov.com**: Dems Want Proof FCC Net Neutrality Page Was Actually Attacked
- **thehill.com**: Dems want independent probe into FCC cyberattack
- **www.schatz.senate.gov**: Letter requesting Investigation (PDF)

Car Safety Vulnerability Lies in the Way CAN Handles Error Messages

(August 16 & 17, 2017)

A vulnerability in the Controller Area Network (CAN) that exists in most new automobiles could be exploited to shut down components of the car, including safety systems. Any component connected to the car's CAN bus could be affected. The issue is not one that can simply be patched because it lies in the CAN bus messaging protocol standard. Components that send too many error messages are disconnected from the CAN, so if attackers can spoof error messages to appear to be coming from a targeted component, that component could be shut off from the CAN.

Editor's Note

[Neely]
To attempt this attack, you have to be connected to the CAN. CAN was designed in 1983 as a stand-alone network; modern electronics have added entry points such as Bluetooth or Wi-Fi. The CAN bus wasn't designed for a flood of error messages; quite the contrary, that's the criterion to indicate a defective component and shut it down to protect the vehicle. While introduction of an IDS/IPS to the CAN could detect an attack, and maybe stop it, it would be hard to tell the difference between an attack and a legitimate malfunctioning component. This reinforces the need for an updated CAN standard designed with more isolation and security necessitated by modern connected components and corresponding threats.

[Northcutt]
Once an attacker accesses the CAN it is game over. A big question is how do they access it, but every security professional needs to understand the basics. I recommend this paper as a start: www.sans.org: Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering

Read more in:
- **www.wired.com**: A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features
- **www.bleepingcomputer.com**: Unpatchable Flaw Affects Most of Today's Modern Cars
- **www.zdnet.com**: How secure is your car? Unpatchable flaw lets attackers disable safety features

ShadowPad Supply Chain Attack Affects NetSarang Software

(August 15, 16, & 17, 2017)

Kaspersky Lab has detected a backdoor in server management software that is used by hundreds of companies around the world. The backdoor, dubbed ShadowPad, lets attackers download additional malware modules and steal information. NetSarang, which makes the affected software, has addressed the issue. Kaspersky was alerted to ShadowPad when one of its customers noticed suspicious DNS requests originating from a system that is used to process financial transactions. ShadowPad was active between July 17 and August 4, 2017.

Editor's Note

[Williams]
Would your monitoring team would have caught this backdoor? It was stealthy; most in-house monitoring teams would not have caught it. It was active for almost a month before being detected. The damage goes beyond the backdoor being present. Did the attackers move laterally? Exfiltrate data? Table top exercises can help you walk through your response to a similar threat.

Read more in:
- **threatpost.com**: Attackers Backdoor Another Software Update Mechanism
- **usa.kaspersky.com**: ShadowPad: Attackers Hid Backdoor in Software Used by Hundreds of Large Companies Worldwide
- **www.cyberscoop.com**: Bad backdoor found in server software used by financial institutions
- **www.scmagazine.com**: 'ShadowPad' attack sabotaged NetSarang software with backdoor

Tech Companies File Amici Brief in Support of Warrants for Cell Phone Data

(August 15 & 16, 2017)

More than a dozen US tech companies filed an amici brief with the US Supreme Court, voicing their support for strong privacy protections and requiring law enforcement to obtain warrants to access certain data from mobile phones. The brief says that law enforcement currently relies on outdated laws to obtain the warrants, which violate the Fourth Amendment.

Editor's Note

[Neely]
Contrast this to the new feature in iOS 11 which will allow you to discretely and quickly disable TouchID, as well as disabling the reported new facial recognition to unlock the device, alleviating fears over access to devices without entering a passcode. This allows some added access control and mitigates the risk of fake or duplicated biometrics.

Read more in:
- **www.wired.com**: Verizon-Yes, Verizon-Just Stood Up for Your Privacy
- **www.law.com**: Tech Giants File Amici Brief in Supreme Court Case Over Cellphone Data
- **www.aclu.org**: Brief for Technology Companies as Amici Curiae... (PDF)

Maersk Details NotPetya Losses

(August 16, 2017)

Shipping company Maersk says that the NotPetya malware attack earlier this summer will ultimately cost it hundreds of millions of dollars in losses due to "significant business interruption." Maersk accounts for nearly 15 percent of all worldwide shipping.

Editor's Note

[Pescatore]
I'm always suspicious of publicly traded companies estimates of losses due to significant events, (especially for, but not just, cyber attacks) but let's do the math: the three business units of Maersk impacted by NotPetya did about $7.7B in revenue in Q2 2017, with a profit of $239M or 3%. The NotPetya impact estimate would pretty much wipe out an entire quarter of profit - definitely a Board of Directors attention-getter. What I hope the Board really focuses on is that the article quotes the CEO as saying, "he learned that there was nothing that could have been done to stop the attack" - even though many of Maersk's direct competitors managed to do just that.

Read more in:
- **www.theregister.co.uk**: NotPetya ransomware attack cost us $300m - shipping giant Maersk
- **threatpost.com**: Maersk Shipping Reports $300m Loss Stemming from Notpetya Attack

Ukrainian Hacker is Now FBI Witness

(August 16, 2017)

A Ukrainian man who turned himself into police in that country earlier this year has become a witness for the FBI. The hacker, known only by his online handle of Profexer, wrote code that was used in cyberattacks against US, believed to be perpetrated by Russia.

Read more in:
- **www.nytimes.com**: In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking
- **arstechnica.com**: Ukraine malware author turns witness in Russian DNC hacking investigation
- **bobsullivan.net**: Ukrainian malware programmer said to be cooperating with U.S. on Russia election hacking probe
- **thehill.com**: Ukraine hacker cooperating with FBI in Russia probe: report

Carnegie Mellon CERT's Guide to Coordinated Vulnerability Disclosure

(August 16, 2017)

Carnegie Mellon University's Software Engineering Institute at the CERT Coordination Center has published a guide to vulnerability disclosure. It is "not a technical document," says report co-author Art Manion, but rather, it "is about a very human process. What should you do when you find a vulnerability? Who do you tell? What should that person do?"

Editor's Note

[Pescatore]
A well-written document if you are looking to read an 88 page description of "responsible disclosure" renamed "Coordinated Vulnerability Disclosure." Or just read the 27 pages Steve Christey and Chris Wysopal wrote in 2002 "Responsible Vulnerability Disclosure Process" - which still ring true today, and is reference 18 in the looong CMU document.

Read more in:
- **www.cyberscoop.com**: This one matters, too: Carnegie Mellon issues guide to disclosing software vulnerabilities responsibly
- **resources.sei.cmu.edu**: The CERT Guide to Coordinated Vulnerability Disclosure

NIST Releases Security and Privacy Controls Draft

(August 15 & 16, 2017)

The US National Institute of Standards and Technology (NIST) has released Draft Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. NIST is taking comments on the draft through September 12, 2017.

Editor's Note

[Pescatore]
A first look shows mostly readability improvements, but I noticed NIST has removed any prioritization guidance, a big step backwards. The rationale seems to be that prioritization should be done when following the Risk Management Framework but the Critical Security Controls have proven the need for prioritization basic security hygiene across any realistic look at reducing real world risk. Heck, even the Payment Card Industry Data Security Standards have had prioritization guidance for years.

Read more in:
- **fcw.com**: NIST retools security and privacy controls for IoT era
- **www.nextgov.com**: NIST Releases Updated Cyber and Privacy Guidance Draft
- **csrc.nist.gov**: Security and Privacy Controls for Information Systems and Organizations (PDF)

Eight Chrome Extensions Hijacked

(August 15 & 16, 2017)

Hackers have hijacked eight Chrome extensions over the past several months. In all eight cases, hackers used phishing attacks to trick developers into exposing their Chrome developer account credentials. The attackers used the access to push out malicious code to users. The affected extensions are Copyfish, Web Developer 0.4.9, Chrometana 1.1.3, Infinity New Tab 3.12.3, Web Paint 1.2.1, Social Fixer 21.1.1, TouchVPN, and Betternet VPN.

Editor's Note

[Murray]
These are "indicators of compromise." What was compromised was the development process of the authors of the extensions.

[Williams]
Plugins are software and should be part of your threat model. More information here:
www.renditioninfosec.com: Software plugins/extensions should be part of your threat model

Read more in:
- **www.zdnet.com**: Google Chrome under attack: Have you used one of these hijacked extensions?
- **www.bleepingcomputer.com**: Eight Chrome Extensions Hijacked to Deliver Malicious Code to 4.8 Million Users
- **threatpost.com**: Seven More Chrome Extensions Compromised

Cyberespionage Group Targeting US Defense Companies

(August 15 & 16, 2017)

A cyber espionage group known as the Lazarus group has been targeting computer systems at US defense contractors, according to Palo Alto Networks. The group, which reportedly has ties to North Korea, was also behind the 2014 attack on Sony Pictures.
Read more in:
- **www.bleepingcomputer.com**: North Korean Cyberspies Target US Defense Contractors Following Nuclear Threats
- **www.v3.co.uk**: North Korea's Lazarus hacking group targets US defence contractors

Malicious PowerPoint Delivered in Spear Phishing Campaign Infected Machines with RAT

(August 15, 2017)

Attackers are exploiting a vulnerability in Microsoft Office to create malicious PowerPoints that place malware in targeted computers. Microsoft released a fix for the flaw in April. The PowerPoint attacks arrive through spear phishing campaigns aimed largely at employees of electronics manufacturing companies. The PowerPoints attempt to infect computers with a Remote Access Trojan (RAT) known as REMCOS.
Editor's Note

[Neely]
This is another attempt to exploit CVE-2017-0199 via a Phishing campaign. While Microsoft published a patch in April, some enterprises have yet to deploy the fix, particularly those in regulated environments where significant regression testing is required before making any changes. I have seen multiple studies that show an interval of 30-200+ days to deploy patches for known vulnerabilities, and this attack leverages this window. Mitigations include more rapid application of patches, quality user awareness training and deployment of modern threat detection and response capabilities.
Trend Micro write up:
blog.trendmicro.com: CVE-2017-0199: New Malware Abuses PowerPoint Slide Show

Read more in:
- **www.scmagazine.com**: Malicious PowerPoint Slide Show files exploit Microsoft bug to deliver REMCOS RAT

Internet Storm Center Tech Corner

Malspam Pushing Trickbot Banking Trojan
https://isc.sans.edu

ShadowPad Backdoor in NetSarang Equipment
https://securelist.com

Banker Google Chrome Extension Targeting Brazil
https://isc.sans.edu

DJI "Go" App May Be Using JSPatch to Modify Applications After Install
https://www.rcgroups.com

Smartlocks Bricked After Auto-Update
http://www.securitysales.com

Analysis of a Paypal Phishing Kit
https://isc.sans.edu

Solving Captcha Audio Challenges (PDF)
http://uncaptcha.cs.umd.edu

Maldoc with auto-updated link
https://isc.sans.edu

Rowhammer is Back: SSD Memory Affected (PDF)
https://www.usenix.org

Nathaniel Quist: Active Defense in a Labyrinth of Deception
https://www.sans.org

The Editorial Board of SANS NewsBites

Alan Paller
Brian Honan
David Hoelzer
David Turley
Dr. Eric Cole
Ed Skoudis
Eric Cornelius
Gal Shpantzer
Jake Williams
Dr. Johannes Ullrich
John Pescatore
Mark Weatherford
Mason Brown
Michael Assante
Rob Lee
Sean McBride
Shawn Henry
Stephen Northcutt
Suzanne Vautrinot
Tom Liston
William Hugh Murray

SANS Institute
8120 Woodmont Avenue, Suite 310, Bethesda, MD, 20814

To create a SANS Portal Account visit create new account.
To change your email address visit update profile.
To change your email preferences or unsubscribe visit manage subscriptions.

Privacy Policy.